Mohamed Bourennane*, Anders Karlsson, and Gunnar Björk
Department of Microelectronics and Information Technology,
Royal Institute of Technology (KTH), Electrum 229, SE-164 40 Kista, Sweden

Nicolas Gisin
GAP-Optique, Universite de Geneve, 20 rue de
l'Ecole de Medecine, 1211 Geneve 4, Switzerland

Nicolas J. Cerf
Ecole Polytechnique, CP 165, Université Libre de Bruxelles, B-1050 Bruxelles, Belgium
and Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91109

(June 11, 2001)

We present security proofs for a protocol for Quantum Key Distribution (QKD) based on encoding in finite high-dimensional Hilbert spaces. This protocol is an extension of Bennett's and Brassard's basic protocol from two bases, two state encoding to a multi bases, multi state encoding. We analyze the mutual information between the legitimate parties and the eavesdropper, and the error rate, as function of the dimension of the Hilbert space, while considering optimal incoherent and coherent eavesdropping attacks. We obtain the upper limit for the legitimate party error rate to ensure unconditional security when the eavesdropper uses incoherent and coherent eavesdropping strategies. We have also consider realistic noise caused by detector's noise.

I. INTRODUCTION

Quantum cryptography aims to provide an *unconditionally* secure key distribution between two parties, Alice and Bob. In the first protocol proposed by Bennett and Brassard (BB84) [1], to detect eavesdropping, Alice and Bob choose randomly between two complementary (conjugate) bases and in each basis the "information" is encoded using two orthogonal quantum states (qubits). Since the basis is unknown to the eavesdropper (by convention called Eve), she cannot simply copy the sent states because the non-cloning theorem. The use of random complementary bases furthermore implies that if the sender Alice prepares a state in one basis, the outcome of a measurement by Bob or Eve in a complementary basis will yield a totally random measurement outcome. These features guarantee that any eavesdropping attempt will invariably introduce errors in the transmission, which can be detected by the legitimate communicating parties. An extension to the BB84 protocol was made by Bruß [2] and by Bechmann-Pasquinucci and Gisin [3] to a six-state, three complementary bases protocol. The analysis shows that Eve's information gain for a given impaired error rate is lower than in the BB84 protocol [2,3]. Very recently two other extensions were proposed where the authors have considered schemes using four states and two bases [4], and three states and four bases [5]. In an earlier work we have generalized these results to encoding in N-dimensional Hilbert space using $M \leq N + 1$ bases [6] where we have considered some specific and rather simple, but realistic, eavesdropping attacks. The goal of this work is to find an ultimate and practical condition for the security of quantum key distribution protocols, sufficiently general to encompass all possible types of eavesdropping. The condition we derive is given in the form of a theorem. We will also derive the upper permissible limit for Bob's error rate to ensure unconditional security when Eve uses incoherent and coherent eavesdropping attacks.

The paper is organized as follows: In Sec. 2, we give a brief introduction to our protocol. In Sec. 3 we reiterate the secrecy capacity of a channel and derive the results for an intercept-resend eavesdropping attack. In Secs. 4 and 5, we study optimal individual eavesdropping attacks, and coherent eavesdropping attacks, respectively. In Sec. 6 we consider realistic systems where we assume that the detector dark count probability is not negligible. Finally, in Sec. 7 we present our conclusions.

*Electronic address: boure@ele.kth.se

II. A MULTI BASES MULTI STATE QUANTUM KEY DISTRIBUTION PROTOCOL

In the BB84 protocol [1], Alice first randomly chooses between one of two bases to prepare her state, and secondly she randomly decides which of two orthogonal states in the chosen basis to send. Extending this protocol to a N-dimensional Hilbert space $\mathcal{H}_N$, Alice first chooses from which of M complementary bases to choose her state from, and secondly she decides which of the N orthogonal states defining the basis to send. The "information" encoded by the chosen state will from hereon be denoted quNits. Each symbol sent in the M bases and N quNits are chosen randomly with equal probability, i.e. each of the possible NM states appear with probability $1/(MN)$. We first define the bases $\{\psi_A\}$ and $\{\psi_B\}$ over an N-dimensional space to be *mutually complementary* if the inner products between all possible pairs of vectors, with one state from each basis, have the same magnitude:

$$|_A\langle\,\psi_i\,|\,\psi_j\,\rangle_B| = 1/\sqrt{N} \qquad \forall \quad i,j. \tag{1}$$

If a quantum state is prepared in the $\{\psi_A\}$ basis, but measured in the complementary $\{\psi_B\}$ basis, the outcome is completely random. Wootters and Fields have shown [7] that when $N = p^k$, where p is a prime and k a positive integer, which we restrict ourselves to here, then there exist a set of $M = N + 1$ mutually complementary bases [7].

To estimate the mutual information between Alice and Bob, Alice and Eve, and the information gain of the eavesdropper Eve, the relevant information measure is the Shannon information of the *sifted* symbols, i.e., the symbols for which Alice and Bob have used the same bases. For simplicity, we choose to measure this information in bits. From the receiver's (Bob's or Eve's) point of view, there will be an *a priori* $p(x)$ and an *a posteriori* $p(x|y)$ probability, the latter being the conditional probability of the sending party (Alice) having sent the symbol x, given that the receiver (Eve or Bob) measured the result y. The receiver's mean information gain from Alice's symbol, I^N_{AY}, where $Y = B, E$ denote either Bob or Eve, equals his or her entropy decrease:

$$I^N_{AY} = H^N_{apri} - H^N_{apost}. \tag{2}$$

The *a priori* probability for Alice's symbol is uniform (since the protocol dictates that Alice must chose the symbols she sends randomly), leading to $H^N_{apri} = \log(N)$. The *a posteriori* entropy is defined:

$$H^N_{apost} = \sum_y p(y) \sum_x p(x|y) \log(p(x|y)), \tag{3}$$

where the *a posteriori* probability of symbol y given observer's result x is given by Bayes' theorem:

$$p(x|y) = \frac{p(y|x)p(x)}{p(y)}, \tag{4}$$

with $p(y) = \sum_x p(y|x)p(x)$.

The mutual information between Bob and Alice as function of Bob's error rate is obtained by using Eq. (2) and by using the symmetry properties of the protocol, i.e., that Bob's measurement errors are independent of, and uniform for, all symbols sent by Alice:

$$I^N_{AB}(e^N_B) = \log(N) + (1 - e^N_B)\log(1 - e^N_B) + e^N_B \log(\frac{e^N_B}{N-1}), \tag{5}$$

where e^N_B is Bob's error rate, i.e., the probability that he measures a symbol erroneously. Note that since expressions (2) and (5) refer to the information and errors contained in the sifted symbols, these errors are due to a possible eavesdropping disturbance and system noise such as the dark counts of the detectors, the tranmission loss, etc. They are not due to Bob's random choice of measurement basis.

III. EAVESDROPPING

In an ideal system, after the quNit string has been transmitted, measured, and sifted, Alice and Bob will share a common key. However, in real systems there are always some errors, and some of these errors may be due to an eavesdropper. Hence, Alice and Bob need to use error correction through a classical channel to establish an identical key, and privacy amplification to obtain a secret common key [8,9]. The eavesdropping attacks by Eve must introduce errors. As stated above this is due to Alice's random choice of measurement basis and the fact that Eve cannot copy an unknown state perfectly. In the case of simple intercept-resend eavesdropping attacks, Eve gets one of the NM possible results. After Alice and Bob announced their choice of bases we have $p(x = y|\{\psi_A\} = \{\psi_E\}) = 1$, $p(x \neq y|\{\psi_A\} = \{\psi_E\}) = 0$, and $p(y|\{\psi_A\} \neq \{\psi_E\}) = 1/N \ \forall \ x, y$. Therefore, according to (2) and (5), Eve's information gain is $I_{AE} = \log(N)/M$ and Bob's error rate becomes $e_B^N = (1 - 1/M)(1 - 1/N)$ when Eve employs the intercept-resend eavesdropping strategy.

Csiszár and Körner [10] have given a lower bound for the *secrecy capacity*, that is, the maximum rate at which Alice can reliably send random symbols to Bob such that the rate at which Eve obtain information about the symbols is arbitrarily small. We can give their result as a theorem, the proof of the theorem is given in [10].

Theorem 1: Alice and Bob can establish a secret key (using error correction and privacy amplification) if, and only if, $I_{AB}^N \geq I_{AE}^N$ or $I_{AB}^N \geq I_{BE}^N$, where I_{AB}^N, I_{AE}^N and I_{BE}^N are the mutual information between Alice and Bob, Alice and Eve, and Bob and Eve, respectively.

Taking the sifting, error correction, and privacy amplification into account, we can hence define an effective transmission rate as

$$R_{AB}^N(e_B^N) = \frac{1}{M}(I_{AB}^N(e_B^N) - I_{AE}^N(e_B^N)). \tag{6}$$

We will discuss in the following sections the different eavesdropping strategies and present a security analysis. First we begin by considering individual attacks where Eve attaches independent probes to each quNit and measures her probes one after the other. Second, we consider coherent attacks in which Eve process several quNits jointly.

IV. INDIVIDUAL EAVESDROPPING ATTACKS: UNIVERSAL QUANTUM CLONING MACHINE

Here we discuss eavesdropping from the perspective of quantum cloning. The basic idea is that Eve uses a quantum information distributor suggested by Braunstein *et al.* [11], or an Universal Quantum Cloning Machine (UQCM), introduced by Bužek and Hillery [12], to obtain two copies of Alice's quantum state, keeping one of the copied states for herself and passing the other copy to Bob. Then, after Bob and Alice have made their measurements and announced their chosen bases, Eve does the same measurement as Bob did, i.e., she measures in the same basis as Alice and Bob, and therefore on the average, she will obtain similar information as Bob. If she uses a UQCM she can also make a coherent measurement on the state of the cloning machine and her copy and then also know if, and when, she introduced an error for Bob [3]. For increasing disturbance, the fidelity F_B between the sent state and the state inferred by Bob (defined on the sifted symbols), that govern the probability that he and Alice will accept the transmitted state, decreases, while Eve's probability of guessing the symbol correctly increases.

Let us analyze the situation when Eve uses a quantum information distributor as a "copying machine". The machine works as follows [13]: If Alice sends the state $|\psi_k\rangle$. The output quantum states of the quantum information distributor are given by:

$$|\psi_k\rangle_A \rightarrow \sum_{m,n} a_{m,n} U_{m,n} |\psi_k\rangle_B |\Psi_{m,-n}\rangle_{EM} \tag{7}$$

where A, B, E and M stand for Alice, Bob, Eve and cloning machine respectively. $a_{m,n}$ (with $m, n = 0, ..., N-1$ and $\sum_{m,n} | a_{m,n} |^2 = 1$) characterize the cloning machine and the quantum states $|\Psi_{m,-n}\rangle_{EM}$ are the generalisation of the Bell states, which are a set of N^2 maximally-entangled (ME) states of two N-dimensional systems, E and M:

$$|\Psi_{m,n}\rangle_{EM} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \mathrm{e}^{2\pi i(jn/N)} |\psi_j\rangle_E |\psi_{j+m}\rangle_M \tag{8}$$

where the indices m and n $(m, n = 0, \cdots, N-1)$ label the N^2 states. Note that, here and below, the ket labels are taken modulo N. It is easy to check that the $|\psi_{m,n}\rangle$ are orthonormal and form a complete basis in the product Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$. $U_{m,n}$ are a group of error operators on a N-dimensional state. In such a channel, an arbitrary state $|\psi\rangle$ undergoes a particular unitary transformation (or error)

$$U_{m,n} = \sum_{k=0}^{N-1} \mathrm{e}^{2\pi i(kn/N)} |\psi_{k+m}\rangle\langle\psi_k| \tag{9}$$

Note that $U_{0,0} = \mathbb{1}$, implying that $|\psi\rangle$ is left unchanged with probability $p_{0,0}$. These error operators generalize the Pauli matrices for qubits: m labels the "shift" errors (generalizing the bit flip σ_x) while n labels the phase errors (generalizing the phase flip σ_z).
In the case of the universal cloner

$$a_{m,n} = \alpha \delta_{m,0} \delta_{n,0} + \frac{\beta}{N} \tag{10}$$

with the normalisation relation:

$$\alpha^2 + \frac{2}{N} \alpha\beta + \beta^2 = 1. \tag{11}$$

Using the above relations and the following relation

$$\sum_{n=0}^{N-1} \mathrm{e}^{2\pi i [(j-j')n/N]} = N\, \delta_{j,j'} \tag{12}$$

After some simple algebra, it is easy to obtain

$$\begin{aligned} \mid \psi_k\rangle_A \to & \sum_m |\psi_{k+m}\rangle_B \left\{ \frac{\alpha}{\sqrt{N}} \delta_{m,0} \sum_l \mid \psi_l\rangle_E \mid \psi_l\rangle_M + \frac{\beta}{\sqrt{N}} \mid \psi_k\rangle_E \mid \psi_{k+m}\rangle_M \right\} \\ & = \mid \psi_k\rangle_B \left\{ \frac{\alpha}{\sqrt{N}} \sum_l \mid \psi_l\rangle_E \mid \psi_l\rangle_M + \frac{\beta}{\sqrt{N}} \mid \psi_k\rangle_E \mid \psi_k\rangle_M \right\} \\ & + \sum_{m\neq 0} \mid \psi_{k+m}\rangle_B \frac{\beta}{\sqrt{N}} \mid \psi_k\rangle_E \mid \psi_{k+m}\rangle_M \end{aligned} \tag{13}$$

. Eve' strategy:
(i) $m = 0$, then the probability that Eve obtains $\mid \psi_k\rangle$ is:

$$p_{m=0}(\mid \psi_k\rangle) = \frac{(\alpha+\beta)^2}{N}, \tag{14}$$

and the probability that Eve obtains any other $N-1$ possibilities $\mid \psi_l\rangle$ with $l \neq k$ is:

$$p_{m=0}(\mid \psi_l\rangle) = \frac{\alpha^2}{N}. \tag{15}$$

(ii) $m \neq 0$, then the probability that Eve obtains $N-1$ of $\mid \psi_k\rangle$ is:

$$p_{m\neq 0}(\mid \psi_k\rangle) = \frac{\beta^2}{N}. \tag{16}$$

The fidelity of Bob is given by

$$\begin{aligned} F_B &= p_{m=0}(\mid \psi_k\rangle) + \sum_{l\neq k} p_{m=0}(\mid \psi_l\rangle) \\ &= \frac{(\alpha+\beta)^2}{N} + (N-1)\frac{\alpha^2}{N} \end{aligned} \tag{17}$$

The mutual information between Alice and Eve is

$$I(A:E \mid m=0) = \log(N) - H_N \left[\frac{(\alpha+\beta)^2}{NF_B}, \frac{\alpha^2}{NF_B}, ..., \frac{\alpha^2}{NF_B} \right], \tag{18}$$

and

$$I(A:E \mid m \neq 0) = \log(N). \tag{19}$$

The total mutual information between Alice and Eve is

$$\begin{aligned}I(A:E) &= F_B I(A:E\mid m=0)+\frac{1-F_B}{N-1}(N-1)I(A:E\mid m\neq 0)\\ &= \log(N)-F_B H_N\left[\frac{(\alpha+\beta)^2}{NF_B},\frac{\alpha^2}{NF_B},...,\frac{\alpha^2}{NF_B}\right]\\ &= \log(N)+\frac{(\alpha+\beta)^2}{N}\log\left[\frac{(\alpha+\beta)^2}{NF_B}\right]+\frac{N-1}{N}\alpha^2\log\left[\frac{\alpha^2}{NF_B}\right].\end{aligned}\tag{20}$$

The total mutual information between Alice and Bob is

$$\begin{aligned}I(A:B) &= \log(N)-H_N\left[F_B,\frac{1-F_B}{N-1},...,\frac{1-F_B}{N-1}\right]\\ &= \log(N)+F_B\log\left[F_B\right]+(1-F_B)\log\left[\frac{1-F_B}{N-1}\right].\end{aligned}\tag{21}$$

As shown in [12] the maximal fidelity of copying a quNit is obtained using the UQCM. This maximal value of the fidelity correspond precisely to the fidelity of optimal incoherent eavesdropping strategy, as Gisin and Bechmann-Pasquinucci have shown explicitly for the $(N=2, M=3)$ case [3]. We argue that from the symmetry of the problem it follows that for $M=N+1$, the fidelity of the optimal incoherent eavesdropping is accomplished using a UQCM.

In Fig. 1, we plot the information rate R^N_{AB}, defined by Eq. (6), as a function of Bob's error rate for different values of N. For each N, the intersection between the graphs R^N_{AB} and the horizontal axis correspond to the upper permissible bound for Bob's error rate to enable secure key distribution. In all cases, the UQCM gives the best performance (from the viewpoint of the eavesdropper) so Alice and Bob should use the UQCM model to estimate the "leakage" of information to Eve when applying privacy amplification.

V. COHERENT EAVESDROPPING ATTACKS

In the previous section we have assumed only individual attacks, i.e., that Eve manipulates and performs measurements on each quNit separately. In this section we address the question: If Eve manipulates several quNits coherently, means an arbitrary large but finite number of quNits. We like to stress that the length of key must be much longer than this number. What is the maximum rate of errors detected by Bob that allows Alice and Bob to still apply error correction and privacy amplification to extract a secure key? Already in 1996, Mayers presented ideas on how to prove this bound [15]. Now several proofs exist [15–18]. Here we shall present the proof in form quite different from the previous ones. We present our result in the form of a theorem:

Theorem 2: In N-dimensional Hilbert space, two users Alice and Bob can establish a secret key if, and only if, Bob's error rate satisfy the inequality:

$$(1-e^N_B)\log(1-e^N_B)+e^N_B\log(\frac{e^N_B}{N-1})\leq-\frac{1}{2}\log(N),\tag{22}$$

where e^N_B is Bob's error rate.

To prove this theorem we need another theorem due to Hall [14] that sets a limit on the sum of the mutual information between Alice and Bob and the mutual information between Alice and Eve.

Theorem 3: Let $\hat{B}$ and $\hat{E}$ be symbol observables for Bob and Eve, respectively, in a N-dimensional Hilbert space such that the maximum possible overlap between any two eigenvectors $|\,\psi_i\,\rangle_B$ and $|\,\psi_j\,\rangle_E$ corresponding to these observables is $C=\mathrm{Max}_{i,j}\{|_B\langle\,\psi_i\,|\,\psi_j\,\rangle_E|\}$. Then the mutual information Alice-Bob and Alice-Eve satisfy the following inequality:

$$I^N_{AB}+I^N_{AE}\leq 2\log_2(NC).\tag{23}$$

Now we are ready to prove Theorem 2.

Proof of Theorem 2: Suppose Alice sent a large number of quNit symbols, and that Bob performed this measurement on n quNits of them using the correct basis. The Hilbert space dimension of the total sifted symbol space is thus N^n. Let us now re-label the bases for each of the n quNits such that, by definition, Alice used all n times the $\{\psi_B\}$ basis. Hence, using this re-labeling, Bob's observable is the n-time tensor product $\hat{B}_1\otimes...\otimes\hat{B}_n$. Since Eve had no way to know the correct bases, her optimal information on the correct ones is precisely the same as her optimal information on the incorrect ones. Hence, one can bound her information assuming she measures $\hat{E}_1 \otimes ... \otimes \hat{E}_n$ where $\hat{E}_i$ is a complementary observable to $\hat{B}_i$. It follows that $C = N^{-n/2}$. By applying Theorem 3, we obtain the following inequality:

$$I_{AB}^N + I_{AE}^N \leq n \log_2(N) \tag{24}$$

By using the inequality $I_{AB}^N \geq I_{AE}^N$ of Theorem 1 and Eq. (24) and we obtain:

$$I_{AB}^N \leq \frac{n}{2} \log_2(N). \tag{25}$$

For string of n symbols, the mutual information between Alice and Bob becomes

$$I_{AB}^N(e_B^N) = n(\log(N) + (1 - e_B^N)\log(1 - e_B^N) + e_B^N \log(\frac{e_B^N}{N-1})). \tag{26}$$

Using the Eqs. (25) and (26), we obtain Theorem 2.

In Fig. 2, we plot the upper bound for the Bob's error rate as function of N in the case of the optimal incoherent and coherent eavesdropping attacks. For $N = 2$ we recover the results for coherent attacks the result by Mayers [15,18] $e_B^2 = 11\%$.

VI. REALISTIC SYSTEMS

The attacks presented in the previous sections assume perfect eavesdropping and measurement apparata, and a noise-free channel. In real secret key distribution systems there are several limitations: The sources can emit more than one photon, some photons never get to Bob's detector (channel loss), the detector quantum efficiency is limited, and the dark count probability (counts not produced by photons) of the detectors is not negligible. We therefore define an experimental Quantum Bit Error Rate (QBER) for a N-dimensional Hilbert space where we assume that the optical noise remains negligible even for large N and the only source of noise is the dark count of the detectors. Under these assumptions the $QBER$ is given by:

$$QBER = \frac{P_{incorrect}}{P_{incorrect} + P_{correct}} \approx \frac{P_{incorrect}}{P_{correct}}, \tag{27}$$

where

$$P_{correct} = \mu \eta_D e^{-\alpha L} \frac{1}{M}. \tag{28}$$

In Eq. (28), μ is the average photon number per symbol, η is the detector quantum efficiency, α is the channel attenuation coefficient, L is the transmission length and $q_{basis} = 1/M$ is a factor which depends inversely on the number of bases used in the protocol . The probability of incorrect counts, when we assume that all incorrect counts come from the detectors and they have the same dark count probability, is given by:

$$P_{incorrect} \approx P_{dark}(N-1)\frac{1}{M}, \tag{29}$$

where P_{dark} is the probability of dark counts by detector. The $QBER$ becomes

$$QBER \approx \frac{P_{dark}(N-1)}{\mu \eta e^{-\alpha L}}. \tag{30}$$

In Fig. 3 we plot the information rate R_{AB} as function of the transmission distance. The intersection of the two curves gives the maximal distance allowed between Alice and Bob such they can establish a secret key with typical parameter values $\eta_D = 20$ %, $\alpha = 0.2\ dB/km$, $\mu = 0.1$ and $P_{dark} = 10^{-5}$.

VII. DISCUSSION AND CONCLUSIONS

In this work we have considered an extension of Bennett's and Brassard's seminal quantum key distribution protocol into a N-dimensional Hilbert space. We have obtained bounds on Bob's permissible error rate in the case of individual and coherent eavesdropping attacks, and we have give the limits for the transmission distances in non-ideal systems. Using similar arguments and methods one could also generalize Ekert's quantum cryptographic protocol [19], based on quantum entanglement and the test of Bell inequality to detect the eavesdropping, to a N-dimensional Hilbert space. Recently Kaszlilowski *et al.* have shown [20] that the violation of local realism by two entangled quNits is stronger than the violation for two entangled qubits. We conjecture that this would also imply a higher degree of security in entanglement-based multi-level quantum cryptography.

ACKNOWLEDGMENTS

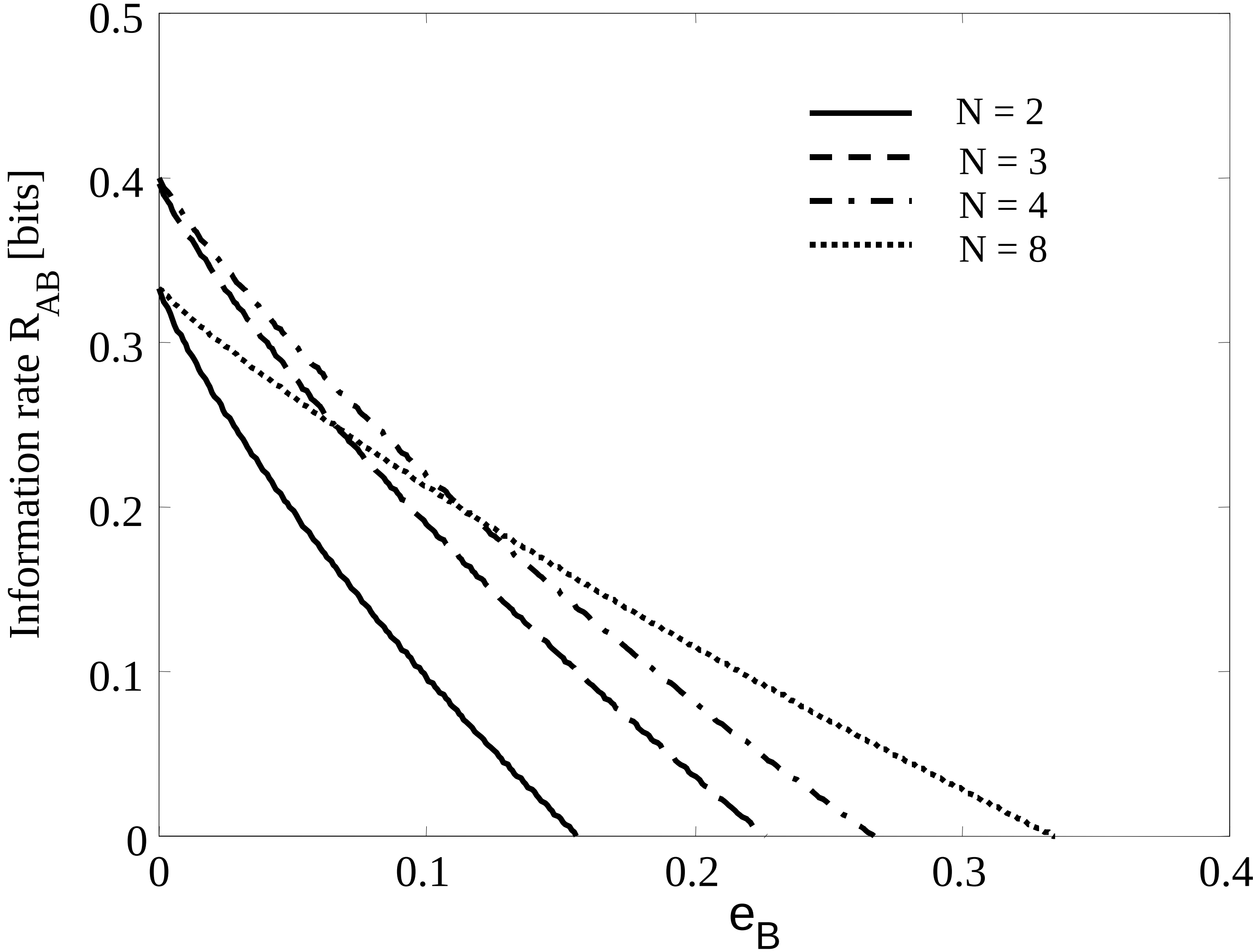
We would like to thank Hugo Zbinden for useful discussions. This work was supported by the Swedish Research Council for Engineering Sciences (TFR), the European Commission through the IST FET QIPC QuComm and EQUIP projects. One of us, M.B., thank GAP-optique for their kind hospitality during his stay there, and the European Science Foundation for financial support.

[1] C. H. Bennett, and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984) 175.
[2] D. Bruss, Phys. Rev. Lett., **81**, 3018 (1998).
[3] H. Bechmann-Pasquinucci, and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[4] H. Bechmann-Pasquinucci, and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[5] H. Bechmann-Pasquinucci, and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[6] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 052313 (2001).
[7] W. K. Wootters, and B. D. Fields, Ann. Phys. **191**, 363, (1989).
[8] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology, **5**, 3 (1992).
[9] C. H. Bennett, G. Brassard, Crepeau, C., and Maurer, U., IEEE Trans. Inf. Theory **41** 1915 (1995).
[10] I. Csiszár, and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[11] S. L. Braunstein, V. Bužek, and M. Hillery, Phys. Rev. A **63**, 052313 (2001).
[12] V. Bužek, and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[13] N. J. Cerf, J. Mod. Opt. **47**, 187 (2000)
[14] M. J. W. Hall, Phys. Rev. Lett. **74**, 3307 (1998).
[15] D. Meyers, J. Assoc. Comput. Math. (to be published), Los Alamos e-print archive, quant-ph/9802025; preliminary version in Advances in cryptography-Proceedings of crypto '96 (Springer-Verlag, New York, 1996), 343.
[16] H.-K Lo, and H. F. Chau, Science **283**, 2050 (1999).
[17] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, In proceedings of the thirty-second Annual ACM Symposium on Theory of Computing (ACM Press, New York, 2000), 715-724.
[18] P. W. Shor, and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[19] A. K. Ekert, Phys. Rev. Lett., **67**, 661 (1991).
[20] D. Kaszlikowski, P. Gnascinski, M. Zukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 1783 (2000).

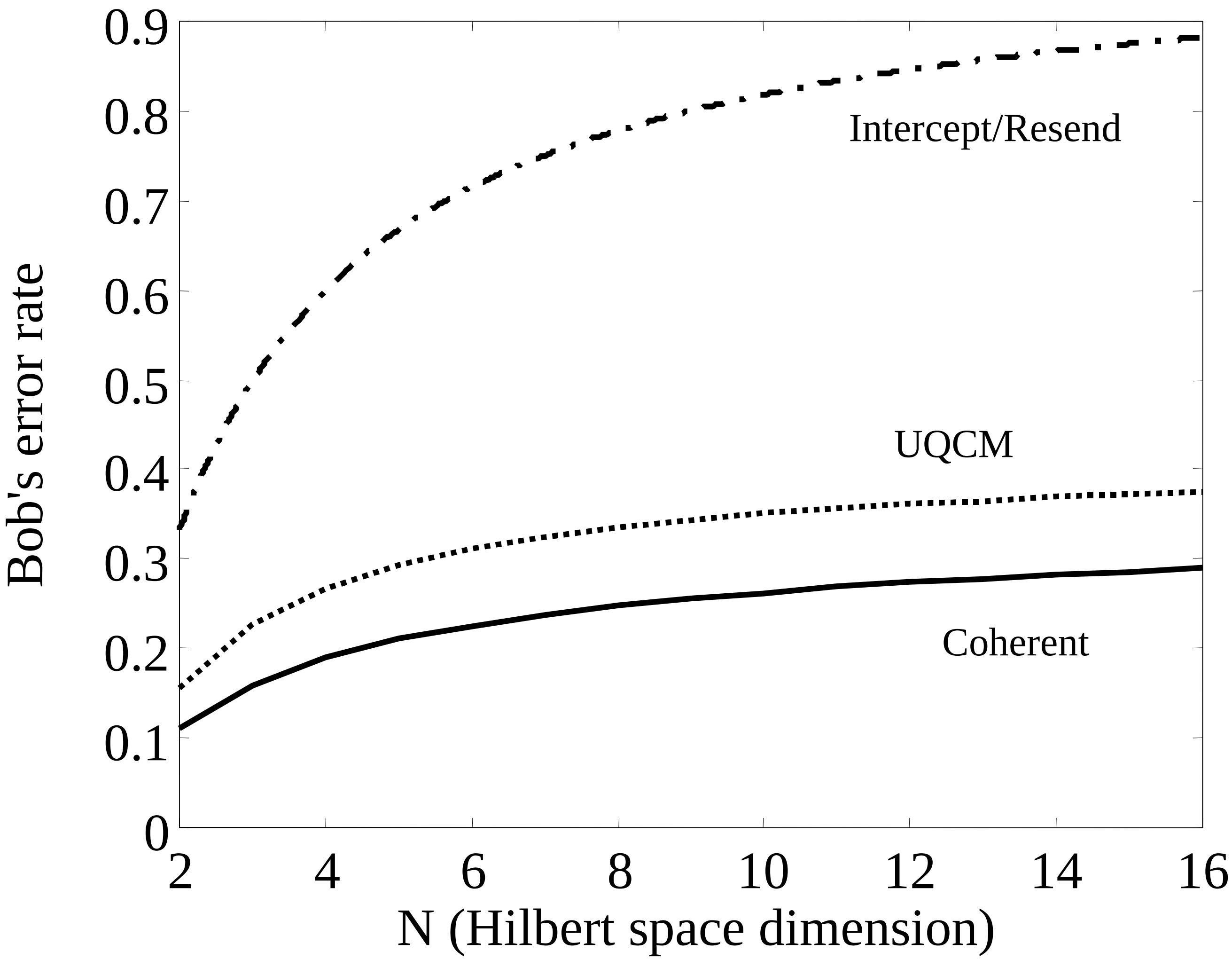
FIG. 1. The information rate R_{AB}, defined by Eq. (6), as a function of Bob's error rate e_B^N for different Hilbert space dimensions N, assuming that $M = N + 1$, using the Universal Quantum Cloning Machine eavesdropping strategy.

FIG. 2. Bob's error rate e_B^N as a function of the dimension of Hilbert space N for optimal incoherent and coherent eavesdropping strategies.

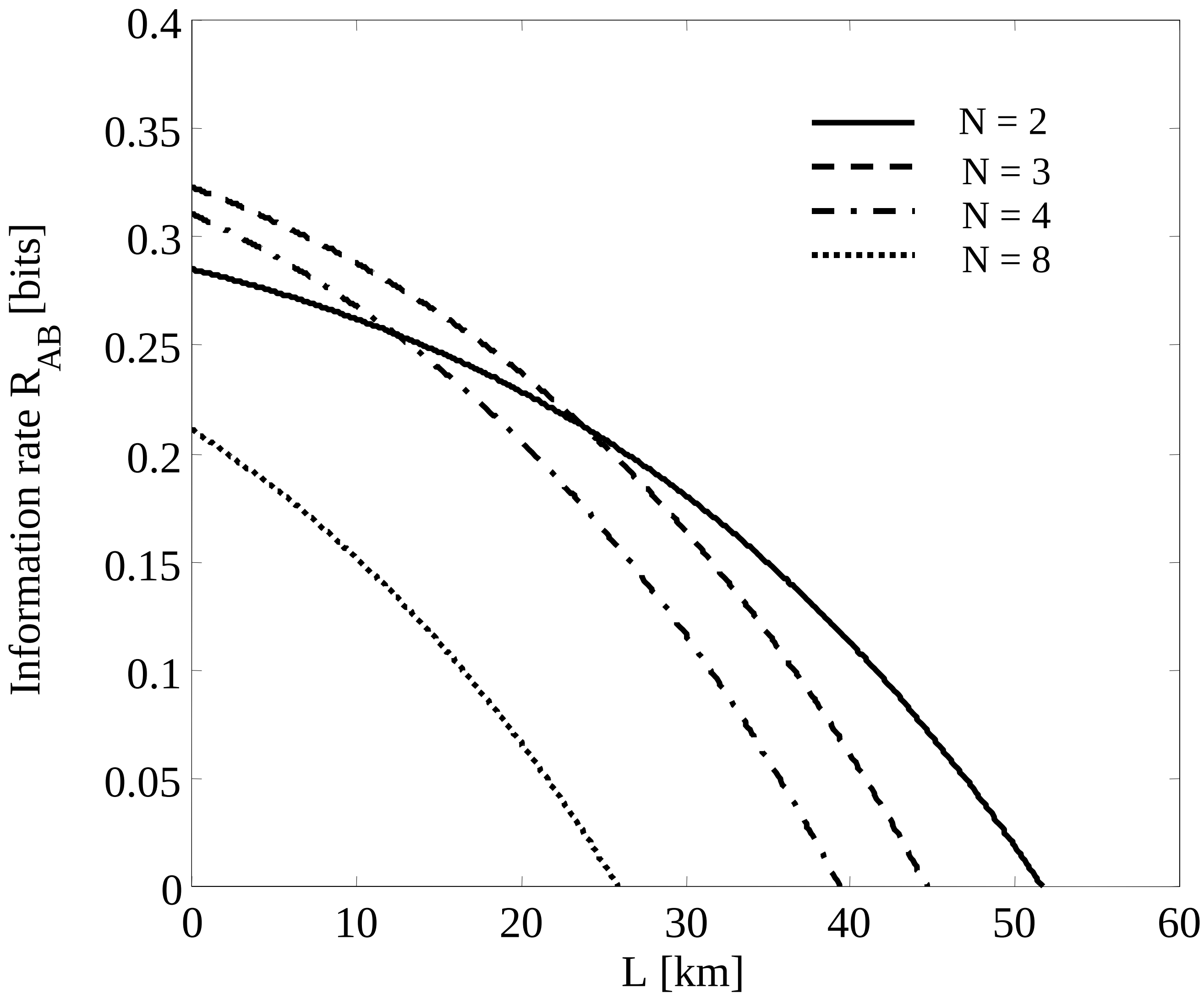
FIG. 3. The information rate R_{AB}, defined by Eq. (6), as a function of the transmission distance L [the distance L is related to the quantum bit error rate by Eq. (30)]. Curves are plotted for different dimensions of the Hilbert space N, assuming that $M = N + 1$ and that the Universal Cloning Machine eavesdropping strategy is used.



0.5
0.4
0.3
0.2
0.1
0
Information rate R_{AB} [bits]
0
0.1
0.2
0.3
0.4
e_B
N = 2
N = 3
N = 4
N = 8



Bob's error rate
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
2
4
6
8
10
12
14
16
N (Hilbert space dimension)
Intercept/Resend
UQCM
Coherent



Information rate R_{AB} [bits]
L [km]
N = 2
N = 3
N = 4
N = 8
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
10
20
30
40
50
60